

# PATENT ABSTRACTS OF JAPAN

Rec'd PCT/PTO KUSANO 16 F022  
10 MAY 2005  
I.D.S. (2)

(11)Publication number : 05-333775

(43)Date of publication of application : 17.12.1993

(51)Int.Cl. G09C 1/00  
G06F 15/16

(21)Application number : 04-142770

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 03.06.1992

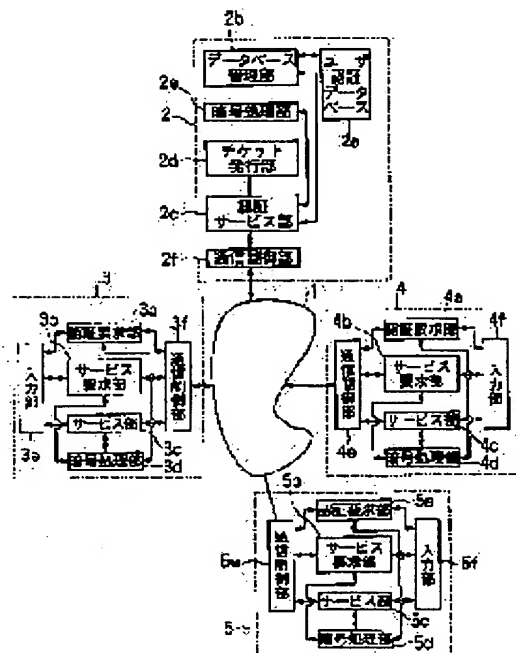
(72)Inventor : SAWA KIMIO  
NUKUI HARUMI

## (54) USER AUTHENTICATION SYSTEM

### (57)Abstract:

PURPOSE: To provide the user authentication system which can be improved in safety and operability than heretofore.

CONSTITUTION: A computer system 2 is equipped with a user authentication database 2a, a database control part 2b which controls the user authentication database 2a, a certifying service part 2c which offers authentication service, a ticket issue part 2d which issues a ticket having a time limit, a ciphering process part 2e which ciphers and composes information, and a communication control part 2f which transmits and receives information through a communication medium 1. Computer systems 3-5 are equipped with certification request parts 3a-5a which sends certification requests to the computer system 2, service request parts 3b-5b which sends service requests to other computer systems, service parts 3c-5c which offer the service, ciphering process parts 3d-5d, input parts 3e-5e, and communication control parts 3f-5f.



## LEGAL STATUS

[Date of request for examination] 12.01.1999

[Date of sending the examiner's decision of rejection] 10.04.2001

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 5 - 3 3 3 7 7 5

(43) 公開日 平成 5 年 ( 1 9 9 3 ) 1 2 月 1 7 日

(51) Int. Cl. <sup>5</sup>

G09C 1/00

G06F 15/16

識別記号

370

庁内整理番号

9194-5L

2 8840-5L

F I

技術表示箇所

審査請求 未請求 請求項の数 1 (全 8 頁)

(21) 出願番号 特願平 4 - 1 4 2 7 7 0

(22) 出願日 平成 4 年 ( 1 9 9 2 ) 6 月 3 日

(71) 出願人 0 0 0 0 0 3 0 7 8

株式会社東芝

神奈川県川崎市幸区堀川町 7 2 番地

(72) 発明者 佐波 公夫

神奈川県川崎市幸区柳町 7 0 番地 株式会  
社東芝柳町工場内

(72) 発明者 貫井 春美

神奈川県川崎市幸区柳町 7 0 番地 株式会  
社東芝柳町工場内

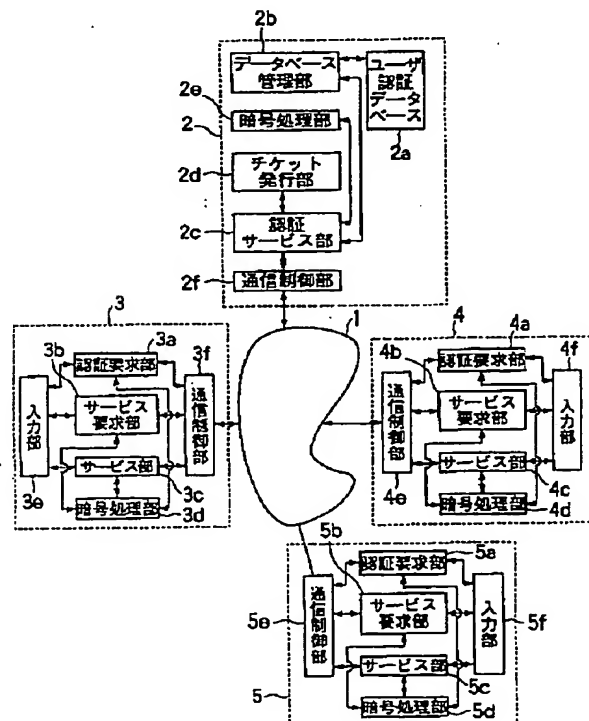
(74) 代理人 弁理士 須山 佐一

(54) 【発明の名称】 ユーザ認証システム

(57) 【要約】

【目的】 従来に較べて安全性の向上と、操作性の向上を図ることのできるユーザ認証システムを提供する。

【構成】 コンピュータシステム 2 は、ユーザ認証データベース 2 a と、ユーザ認証データベース 2 a を管理するデータベース管理部 2 b と、認証サービスを行う認証サービス部 2 c と、時間制限の付いたチケットを発行するチケット発行部 2 d と、情報の暗号化および復合を行う暗号処理部 2 e と、通信媒体 1 を介して情報の送受信を行う通信制御部 2 f とを備えている。コンピュータシステム 3 ~ 5 は、コンピュータシステム 2 に対して認証要求を行う認証要求部 3 a ~ 5 a と、他のコンピュータシステムに対してサービス要求を行うサービス要求部 3 b ~ 5 b と、サービスを実行するサービス部 3 c ~ 5 c と、暗号処理部 3 d ~ 5 d と、入力部 3 e ~ 5 e と、通信制御部 3 f ~ 5 f とを備えている。



## 【特許請求の範囲】

【請求項 1】 複数のコンピュータシステムが通信媒体を介して接続され、これらのコンピュータシステムのファイルや CPU を相互に利用可能に構成されたネットワークシステムのユーザ認証システムにおいて、

前記ネットワークシステムに、前記各コンピュータシステムからのユーザ認証要求に応じて、ユーザ情報を格納する記憶手段を検索してユーザが登録されているか否かを判定し、ユーザが登録されている場合は、ユーザの正当性を制限時間付きで証明するチケットと前記記憶手段に格納されたパスワードとを暗号化して返送する認証用のコンピュータシステムを設けるとともに、前記各コンピュータシステムに、前記通信媒体上での前記ユーザ情報の交換を暗号化する暗号処理手段を設けたことを特徴とするユーザ認証システム。

## 【発明の詳細な説明】

## 【 0 0 0 1 】

【産業上の利用分野】 本発明は、通信媒体を介して有機的に接続された複数のコンピュータシステムから構成されるネットワークシステムのセキュリティシステムにおけるユーザ認証システムに関する。

## 【 0 0 0 2 】

【従来の技術】 近年、任意の通信媒体を介して複数のコンピュータシステムを接続し、これらのコンピュータシステムのファイルや CPU を相互に利用可能としたネットワークシステムが開発されている。

【 0 0 0 3 】 このようなネットワークシステムでは、セキュリティ等のため、コンピュータシステムの利用開始手続や、各種サービスを開始する開始手続の際に、ユーザの認証を行うよう構成されたものが多い。従来、このようなユーザの認証は、利用対象となるコンピュータシステムが、当該コンピュータシステム自身が管理する利用者情報を基に、利用の許可または拒否をその都度判断している。

【 0 0 0 4 】 したがって、認証が必要な他のコンピュータシステムのサービスを利用する場合、利用者が入力したユーザ名やパスワード等の情報は、入力操作を行ったコンピュータシステムから、通信媒体を通して、利用対象となるコンピュータシステムに伝達される。

## 【 0 0 0 5 】

【発明が解決しようとする課題】 上述したように、従来は、コンピュータシステムの利用開始手続等に伴うユーザの認証を、利用対象となるコンピュータシステムが、当該コンピュータシステム自身が管理する利用者情報を基にして実施している。

【 0 0 0 6 】 しかしながら、このようなシステムでは、通信媒体上を利用者の情報（ユーザ名やパスワード等）が第三者に判読可能な形で流れているため、安全上好ましくないという問題があった。また、ネットワーク上の各コンピュータ毎に管理する利用者情報が異なると、利

用者は、利用対象のコンピュータによって利用者識別子（パスワード）等を変えなければならない、操作性が損なわれるという問題もあった。

【 0 0 0 7 】 本発明は、かかる従来の事情に対処してなされたもので、従来に較べて安全性の向上と、操作性の向上を図ることのできるユーザ認証システムを提供しようとするものである。

## 【 0 0 0 8 】

【課題を解決するための手段】 すなわち、本発明は、複数のコンピュータシステムが通信媒体を介して接続され、これらのコンピュータシステムのファイルや CPU を相互に利用可能に構成されたネットワークシステムのユーザ認証システムにおいて、前記ネットワークシステムに、前記各コンピュータシステムからのユーザ認証要求に応じて、ユーザ情報を格納する記憶手段を検索してユーザが登録されているか否かを判定し、ユーザが登録されている場合は、ユーザの正当性を制限時間付きで証明するチケットと前記記憶手段に格納されたパスワードとを暗号化して返送する認証用のコンピュータシステムを設けるとともに、前記各コンピュータシステムに、前記通信媒体上での前記ユーザ情報の交換を暗号化する暗号処理手段を設けたことを特徴とする。

## 【 0 0 0 9 】

【作用】 上記構成の本発明のユーザ認証システムによれば、ネットワークにおけるユーザ情報を認証用のコンピュータシステムによって一元管理するので、パスワード等を統一することができ、従来に較べて操作性の向上を図ることができる。

【 0 0 1 0 】 また、通信媒体には、第三者に判読可能な形でユーザ情報が流れることがなく、さらに、認証に使用されるチケットは時間制限が付いているので第三者に不当に使用される可能性も低減することができ、従来に較べて安全性の向上を図ることができる。

## 【 0 0 1 1 】

【実施例】 以下、本発明の一実施例を、図面を参照して説明する。

【 0 0 1 2 】 図 1 は本発明の一実施例の構成を示すものである。同図において、1 は通信媒体であり、この通信媒体 1 を介して、複数のコンピュータシステム 2、3、4、5 が接続されている。

【 0 0 1 3 】 上記各コンピュータシステムのうち、コンピュータシステム 2 は、ネットワーク上のユーザ情報を一括管理する認証サーバであり、ユーザ情報を格納するユーザ認証データベース 2 a と、このユーザ認証データベース 2 a を管理するデータベース管理部 2 b と、他のコンピュータシステム 3、4、5 からの認証要求を受けて認証サービスを行う認証サービス部 2 c と、サービス時にユーザの利用許可を判断する基となるチケットであって時間制限の付いたチケットを発行するチケット発行部 2 d と、情報の暗号化および復合を行う暗号処理部 2

e と、通信媒体 1 を介して情報の送受信を行う通信制御部 2 f とを備えている。

【 0 0 1 4 】 また、コンピュータシステム 3、4、5 は、ユーザが一般に利用するコンピュータであり、コンピュータシステム 2 に対して認証要求を行う認証要求部 3 a、4 a、5 a と、他のコンピュータシステムに対してサービス要求を行うサービス要求部 3 b、4 b、5 b と、サービスを実行するサービス部 3 c、4 c、5 c と、前述した暗号処理を行う暗号処理部 3 d、4 d、5 d と、ユーザが入力を行うための入力部 3 e、4 e、5 e と、通信媒体 1 を介して情報の送受信を行う通信制御部 3 f、4 f、5 f とを備えている。

【 0 0 1 5 】 ここで、コンピュータシステム 3 においてユーザが利用を開始し、コンピュータシステム 4 のサービスの利用を開始するまでの手続きを例にして、認証手順を説明する。

【 0 0 1 6 】 まず、コンピュータシステム 3 の利用開始時における初期認証のユーザ認証手順について説明する。図 2 のフローチャートに示すように、まず、ユーザは、コンピュータシステム 3 の入力部 3 e から、認証要求部 3 a に対して、ユーザ名を入力する ( 1 0 0 ) 。

【 0 0 1 7 】 認証要求部 3 a は、通信制御部 3 f により、通信媒体 1 を介してこの入力されたユーザ名をコンピュータシステム ( 認証サーバ ) 2 に送り、ユーザの初期チケットとユーザ認証データベース 2 a に登録されている暗号化されたパスワードを要求する ( 1 0 1 ) 。

【 0 0 1 8 】 コンピュータシステム 2 においては、通信制御部 2 f によって受信したユーザ名を、認証サービス部 2 c に入力し、認証サービス部 2 c はユーザ名をデータベース管理部 2 b に送ってこのユーザ名がユーザ認証データベース 2 a に登録されているか否かをチェックする ( 1 0 2 ) 。

【 0 0 1 9 】 そして、ユーザ名が登録されていれば、チケット発行部 2 d によって所定時間 (例えば数時間乃至十数時間) の時間制限が付いた初期チケットを作成し ( 1 0 3 )、この初期チケットと、ユーザ名に対応してユーザ認証データベース 2 a に登録されているパスワードを、暗号処理部 2 e において暗号化する ( 1 0 4 )。ここで、初期チケットに時間制限を付けるのは、第三者による不正使用を防止するためである。すなわち、初期チケットに時間制限がないと、正当なユーザが認証を受け、初期チケットが発行されて、当該コンピュータシステムを使用した後、この初期チケットによって第三者が当該コンピュータシステムを不正使用する可能性があるからである。

【 0 0 2 0 】 一方、ユーザがユーザ認証データベース 2 a に登録されていない場合は、認証不可とし ( 1 0 5 )、通信制御部 2 f を介して、これらの結果をコンピュータシステム 3 に返送する ( 1 0 6 ) 。

【 0 0 2 1 】 コンピュータシステム 3 では、通信制御部

3 f においてこの結果を受信し、認証要求部 3 a に入力する。認証要求部 3 a では、入力部 3 e からユーザにパスワードの入力を促し、ユーザがパスワードを入力すると ( 1 0 7 )、暗号処理部 3 d においてコンピュータシステム 2 からの送信内容を復号し ( 1 0 8 )、これらのパスワードが一致するか否かを判定する ( 1 0 9 )。ここで、パスワードが一致すればコンピュータシステム 3 は利用可能となり、初期チケットは制限時間の間有効となる。また、パスワードが一致しなければ利用不可となる。

【 0 0 2 2 】 なお、上記使用開始時におけるユーザ認証のプロトコルを、図 5 に示す。同図において、C はコンピュータシステム 3、AS は認証サーバであるコンピュータシステム 2 を示している。

【 0 0 2 3 】 次に、ユーザが、コンピュータシステム 3 からコンピュータシステム 4 のサービスを利用する場合について説明する。

【 0 0 2 4 】 ユーザが、入力部 3 e からサービス要求部 3 b に、コンピュータシステム 4 のサービスを利用したい旨の入力を行うと、図 3 に示すように、まずサービス要求部 3 b は、サービス用の証明書 ( サービスチケット ) があるか否かを調べ ( 2 0 0 )、サービスチケットが無い場合は、コンピュータシステム 2 に対してサービスチケットを要求する ( 2 0 1 ) 。

【 0 0 2 5 】 そして、サービスチケットがある場合は次に ( サービスチケットがない場合はコンピュータシステム 2 からサービスチケットを受け取った後 )、初期チケットが有効期限内か否かを調べ ( 2 0 2 )、有効期限内であれば、暗号処理部 3 d でサービスチケットを暗号化し ( 2 0 3 )、この暗号化したサービスチケットを通信制御部 3 f からコンピュータシステム 4 に送って、サービス要求を行う ( 2 0 4 ) 。

【 0 0 2 6 】 コンピュータシステム 4 では、通信制御部 4 e において、上記サービス要求を受信し、このサービス要求をサービス部 4 c に入力する。サービス部 4 c では、暗号処理部 4 d において送られてきたサービスチケットを復号し ( 2 0 5 )、正しいユーザであるか否かを確認 ( 2 0 6 ) する。そして、正しいユーザである場合はサービスを受理する旨を返送してサービスを開始し、正しいユーザでない場合はサービスを拒否する旨を返送する。

【 0 0 2 7 】 なお、上記サービス時におけるユーザ認証のプロトコルを、図 6 に示す。同図において、C はコンピュータシステム 3、AS は認証サーバであるコンピュータシステム 2、S はサービスを行うコンピュータシステム 4 を示している。

【 0 0 2 8 】 次に、上述したステップ 2 0 1 におけるサービスチケット要求、発行の処理を説明する。

【 0 0 2 9 】 サービスチケットを有しない場合、図 4 に示すように、コンピュータシステム 3 では、まず、暗号

10

20

30

40

50

処理部 3 d において、初期チケットと利用するコンピュータシステム名（コンピュータシステム 4）を暗号化し（300）、これらを通信制御部 3 f からコンピュータシステム 2 に送付して、サービスチケットの発行を要求をする（301）。

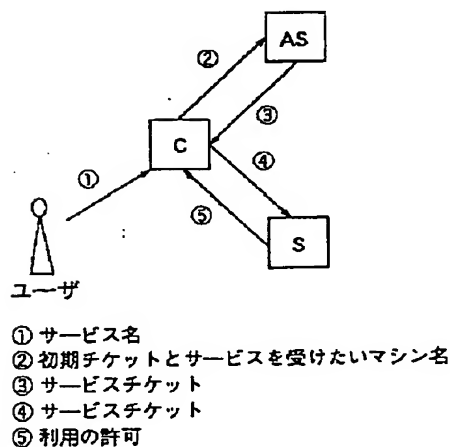
【0030】コンピュータシステム 2 では、通信制御部 2 f においてこの要求を受信し、この要求は、認証サービス部 2 c に入力される。認証サービス部 2 c では、暗号処理部 2 e によって送られてきたデータを復号し（302）、初期チケットが正しいか（時間切れでないか）否かを確認する（303）。

【0031】そして、初期チケットが正しい場合は、チケット発行部 2 d においてサービスチケットを作成し（304）、このサービスチケットを暗号処理部 2 e によって暗号化して（305）、通信制御部 2 f からコンピュータシステム 3 に返送する。また、初期チケットが時間切れの場合等は、その旨をコンピュータシステム 3 に返送する（306）。

【0032】コンピュータシステム 3 では、通信制御部 3 f によってサービスチケットを受信し、このサービスチケットを暗号処理部 3 d によって復号し、格納する（307）。

【0033】このように、本実施例によれば、ネットワークにおけるユーザ情報を認証サーバであるコンピュータシステム 2 によって一元管理するので、パスワード等を統一することができ、従来に較べて操作性の向上を図ることができる。また、通信媒体 1 には、第三者に判読可能な形でユーザ情報が流れることがなく、さらに、認証に使用される初期チケット等は時間制限が付いている

【図 5】



ので第三者に不当に使用される可能性も低減することができる。従来に較べて安全性の向上を図ることができる。

【0034】

【発明の効果】以上説明したように、本発明のユーザ認証システムによれば、従来に較べて安全性の向上と、操作性の向上を図ることができる。

【図面の簡単な説明】

【図 1】本発明の一実施例の構成を示す図。

【図 2】本発明の一実施例における使用開始時のユーザ認証の手順を示す図。

【図 3】本発明の一実施例におけるサービス時のユーザ認証の手順を示す図。

【図 4】本発明の一実施例におけるサービスチケット発行の手順を示す図。

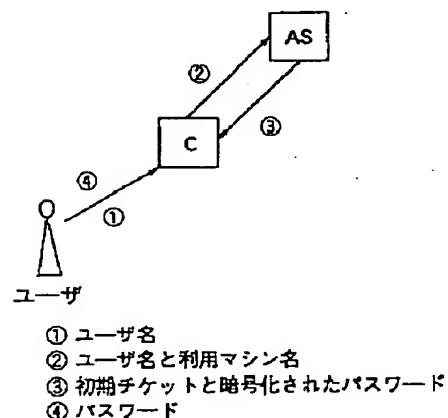
【図 5】使用開始時におけるユーザ認証のプロトコルを示す図。

【図 6】サービス時におけるユーザ認証のプロトコルを示す図。

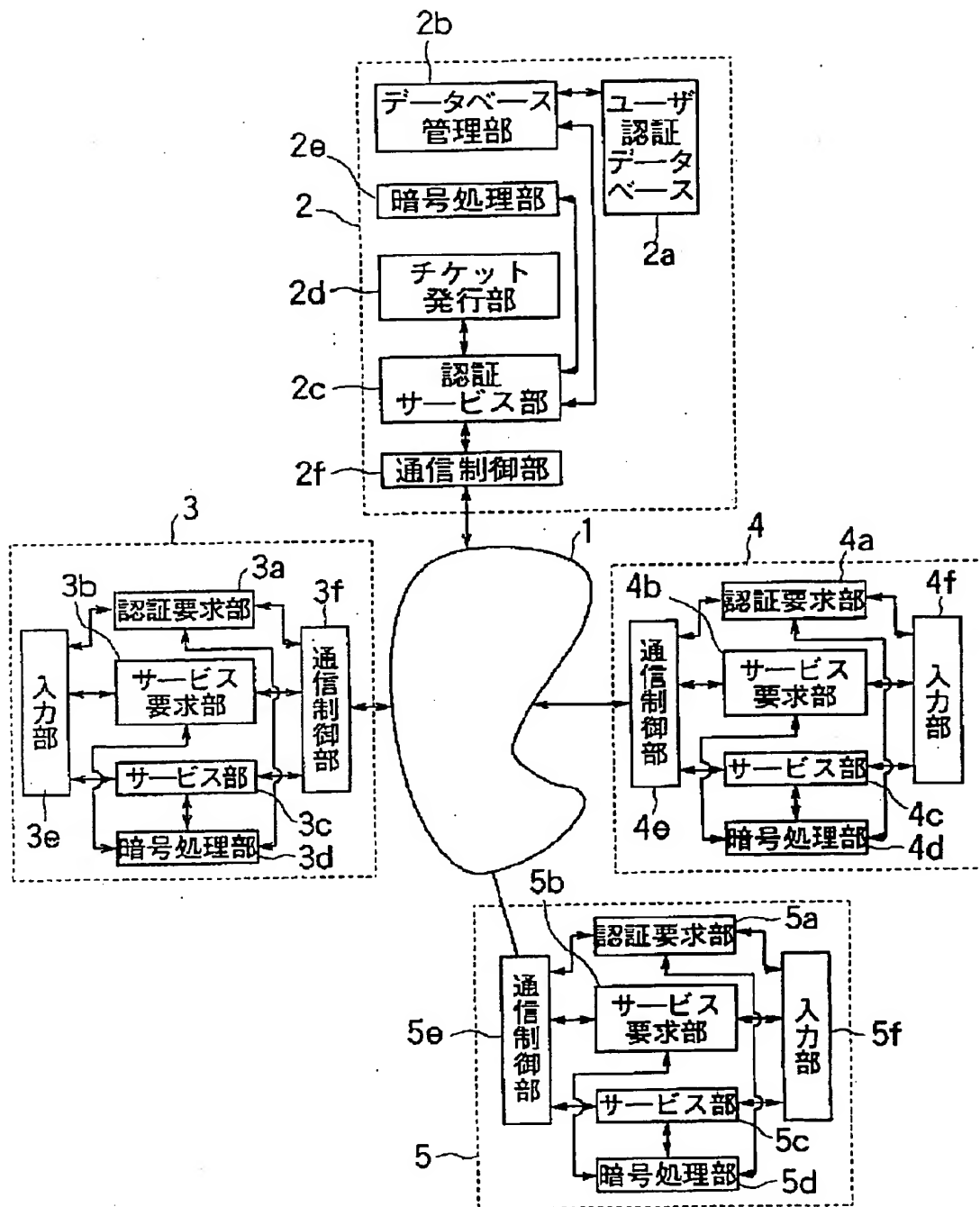
【符号の説明】

- 1 通信媒体
- 2 コンピュータシステム（認証用）
- 2 a ユーザ認証データベース
- 2 b データベース管理部
- 2 c 認証サービス部
- 2 d チケット発行部
- 2 e 暗号処理部
- 2 f 通信制御部
- 3、4、5 コンピュータシステム
- 3 d、4 d、5 d 暗号処理部

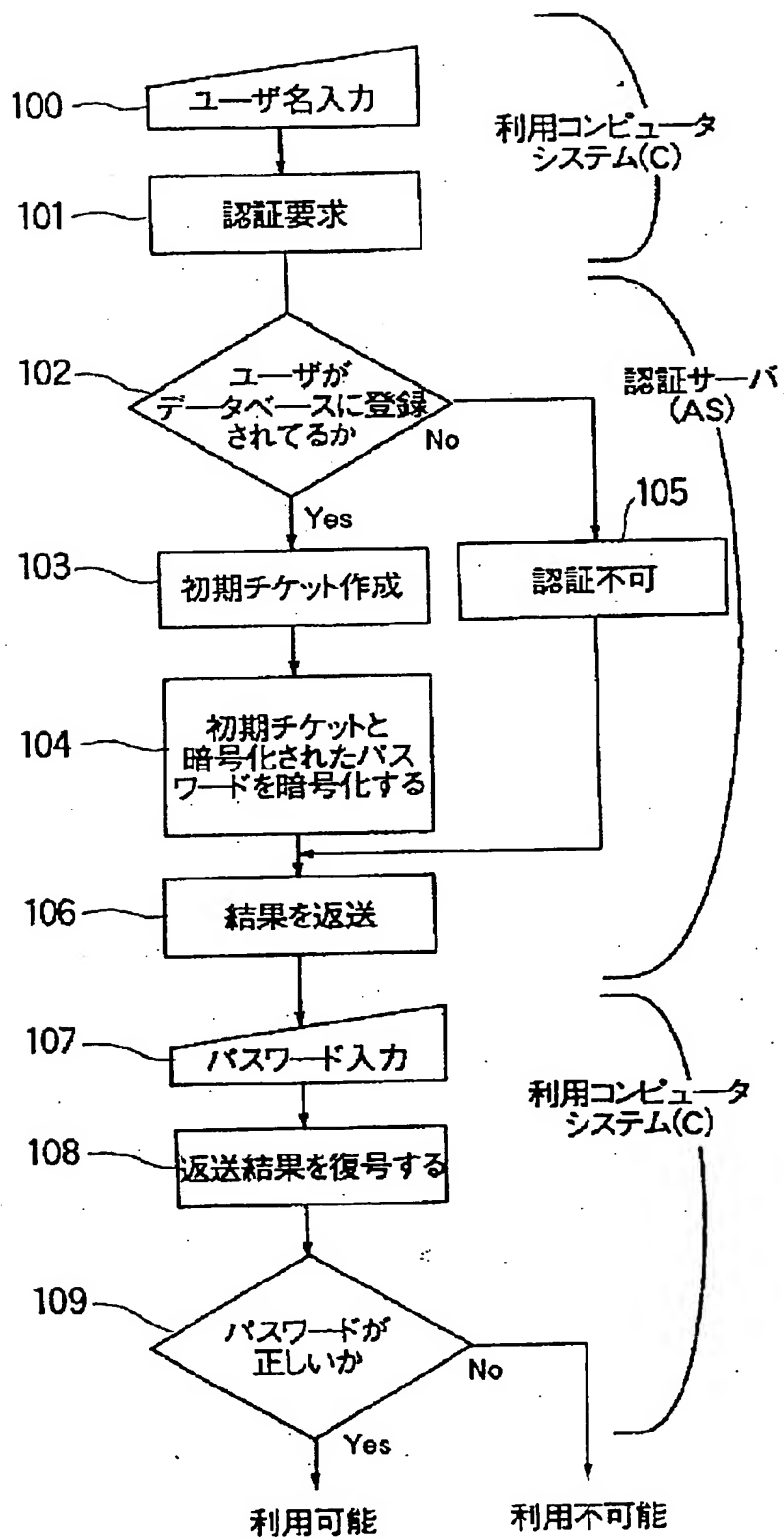
【図 6】



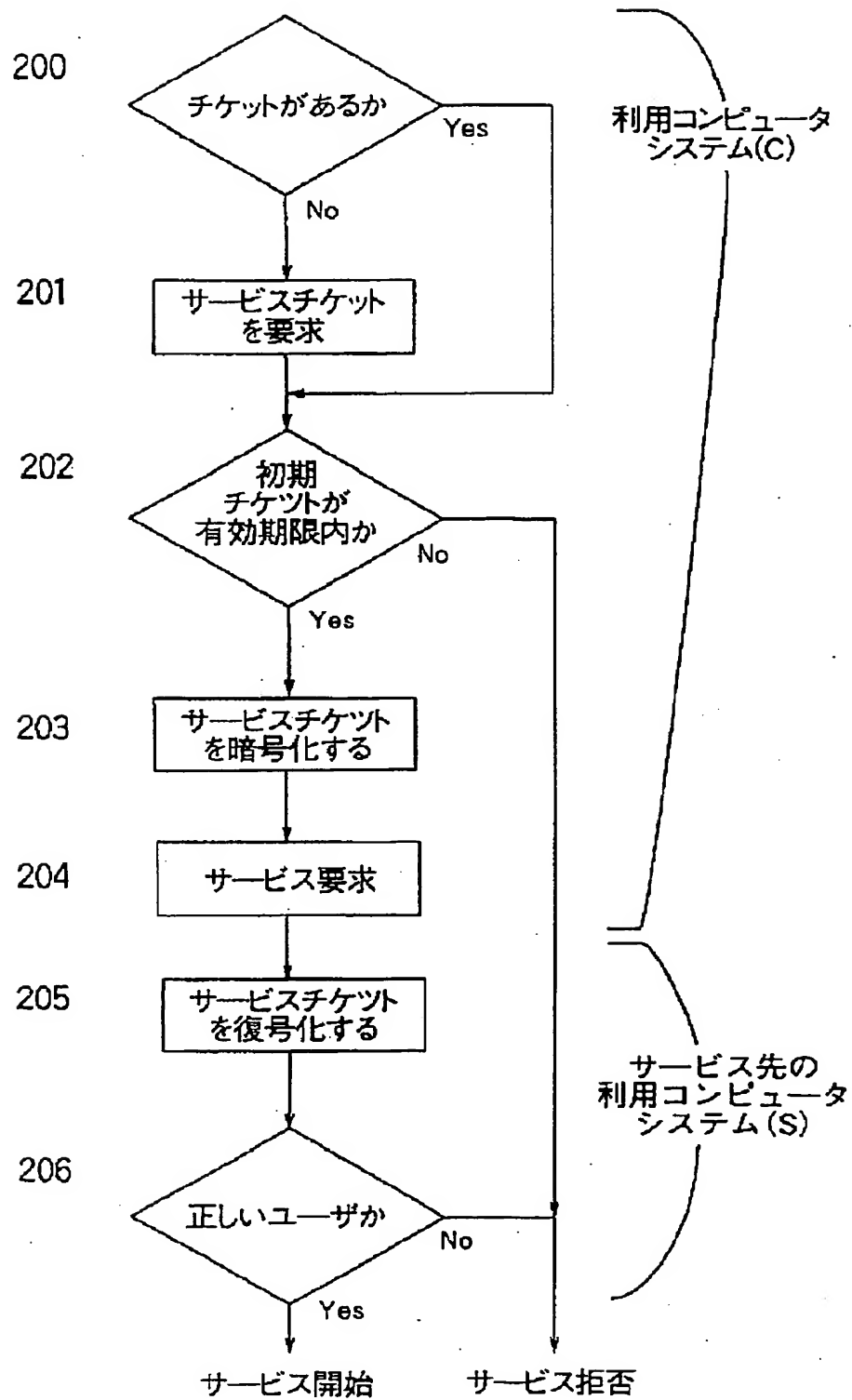
【図 1】



〔図 2〕



【図 3】





〔図 4〕

